TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 700	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00150	Date du dépot international *(jour/mois/année)* 24/01/2000	Date de priorité *(jour/mois/année)* 09/03/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06F11/28		
Déposant GEMPLUS et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 6 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 23/09/2000	Date d'achèvement du présent rapport 27.03.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Bauer, R N° de téléphone +49 89 2399 7477

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00150

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17).*) :

Description, pages:

1-23 version initiale

Revendications, N°:

1-32 reçue(s) le 09/03/2001 avec la lettre du 05/03/2001

Dessins, feuilles:

1/5-5/5 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :
- ☒ des revendications, n[os] : 33-34
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-32
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-32
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-32
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

Concernant le point V

1 L'objet de la **revendication 1** semble être nouveau et inventif.

La **revendication 1** définit un procédé de surveillance du déroulement de l'exécution d'une suite linéaire d'instructions d'un programme.

L'état de la technique le plus proche cité dans la description décrit des procédés de test essayant d'éviter une action malveillante provenant du déroulement erroné du programme. Des actions malveillantes sont, par exemple, la divulgation de données secrètes enregistrées sur une carte à puce ou la manipulation de telles données. Ces procédés changent dans un environnement de test la valeur du compteur d'instruction avec les techniques de modification des calculs ou de sondage. Le compteur d'instruction modifié provoque un déroulement inattendu du programme. Si aucun de ces déroulements inattendus du programme ne cause des actions malveillantes, le déroulement du programme remplit les exigences de sécurité et sera approuvé.

L'état de la technique le plus proche cité par le demandeur utilise la technique de tester quelques valeurs erronées du compteur d'instruction pour décider si le déroulement du programme ne provient d'une action malveillante. Il n'est pas possible de tester toutes les valeurs erronées du compteur d'instruction. Par conséquent, ces procédés de test ne peuvent pas prouver que le déroulement du programme ne provient d'aucune action malveillante.

Le procédé défini dans la **revendication 1** n'utilise pas la technique de test mais au contraire vérifie que la suite linéaire d'instructions d'un programme est exécutée de façon linéaire. La vérification comprend l'extraction d'une donnée de chaque instruction, un calcul prédéterminé sur chaque donnée ainsi extraite et une comparaison du résultat du calcul avec une donnée de référence prédéterminée. Par conséquent, le procédé défini dans la **revendication 1** assure que le déroulement du programme ne provient d'aucune action malveillante.

Aucun des deux documents cités dans le rapport de recherche internationale ne décrit une vérification de l'exécution d'une suite linéaire d'instructions comme défini dans la **revendication 1.**

Donc, l'objet de **la revendication 1** est nouveau et inventif et satisfait aux conditions requises à *l'article 33(2) et 33(3) PCT.*

2 Les **revendications 2-19** sont dépendantes de la **revendication 1** et ajoutent des caractéristiques supplémentaires au procédé inventif de la **revendication 1.** Donc, l'objet des **revendications 2-19** est nouveau et inventif et satisfait aux conditions requises à *l'article 33(2) et 33(3) PCT.*

3 La **revendication 20** porte sur un dispositif dont les caractéristiques techniques sont aux étapes des procédés selon les **revendications 1-19.**
Les **revendications 21-32** ajoutent des caractéristiques supplémentaires au dispositif de la **revendication 20.**
Donc, l'objet des **revendications 20-32** est nouveau et inventif et satisfait aux conditions requises à *l'article 33(2) et 33(3) PCT.*

REVENDICATIONS

1. Procédé de surveillance du déroulement de l'exécution d'une suite linéaire d'instructions (Inst.1-Inst.n) d'un programme informatique, consistant à analyser la séquence des instructions transmises vers le processeur (4) destiné à exécuter le programme surveillé et à vérifier le résultat de cette analyse par référence à des données de référence (Vréf) enregistrées avec ledit programme caractérisé en ce que les données de référence comprennent une valeur (Vréf) préétablie de manière à correspondre au résultat de l'analyse réalisée lors du procédé de surveillance seulement si toutes les instructions (Inst.1-Inst.n) de la séquence d'instructions ont été effectivement analysées lors du déroulement du programme et en ce que ladite analyse de la séquence d'instructions (Inst.1-Inst.n) comprend l'extraction (38) d'une donnée de chaque instruction transmise vers le processeur (4) et un calcul prédéterminé (40, 42) sur chaque donnée ainsi extraite, et en ce que la vérification comprend une comparaison (50) du résultat de l'analyse avec les données de référence (Vréf).

2. Procédé selon la revendication 1, caractérisé en ce que ladite vérification du résultat de l'analyse est provoquée par une instruction (Inst.n+1) placée à un emplacement prédéterminé dans le programme à surveiller, cette instruction contenant les données de référence (Vréf) relatives à un ensemble d'instructions (Inst.1-Inst.n) dont l'exécution correcte est à surveiller.

3. Procédé selon l'une quelconque des revendications 1 à 2, caractérisé en ce que, lorsque les instructions (Inst.1-Inst.n) de l'ensemble d'instructions à surveiller se présentent sous la forme d'une valeur, par exemple des codes enregistrés sous forme hexadécimal ou décimal, on effectue ladite analyse des instructions en considérant celles-ci en tant que valeur numérique.

4. Procédé selon la revendication 1, comprenant les étapes consistant à :

- lors de la préparation du programme à surveiller :
- incorporer, à au moins un emplacement prédéterminé d'une séquence d'instructions (Inst.1-Inst.n) du programme, une valeur de référence (Vréf) établie

selon une règle prédéterminée appliquée sur des données identifiables dans chaque instruction à surveiller, et

- lors de l'exécution du programme à surveiller:

- obtenir (38) lesdites données identifiables dans chaque instruction reçue en vu de son exécution,

- appliquer (40, 42) ladite règle prédéterminée sur lesdites données identifiables ainsi obtenues pour établir une valeur de vérification (VHn), et

- vérifier (50) que cette valeur de vérification correspond effectivement à la valeur de référence enregistrée avec le programme.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comprend en outre une étape (56) d'interruption du déroulement du programme surveillé si l'analyse révèle le programme surveillé ne s'est pas déroulé de manière prévue.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comprend en outre une étape (70) d'invalidation pour usage futur du dispositif comprenant le programme surveillé si ladite analyse révèle un nombre prédéterminé de fois que le programme surveillé ne s'est pas déroulé de manière prévue.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce l'ensemble d'instructions à surveiller ne comporte pas de sauts dans son déroulement prévu.

8. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que, lorsque le programme (EI1, EI2, EI3) ou la portion de programme à surveiller prévoit au moins un saut, on applique le procédé de surveillance séparément sur des ensembles d'instructions de ce programme qui ne comportent pas de sauts entre deux instructions successives.

9. Procédé selon la revendication 8, caractérisé en ce que lorsque le programme à surveiller comporte une instruction (EI1-j) donnant lieu à un saut dépendant des données manipulées, on met en œuvre le procédé de surveillance

séparément pour un ensemble d'instructions (EI1) qui précède le saut, et pour au moins un ensemble d'instructions (EI2, EI3) qui succède à ce saut.

10. Procédé selon la revendication 9, caractérisé en ce que, pour un ensemble d'instructions (EI1) prévoyant un saut, on intègre à cet ensemble l'instruction (EI1-j) qui commande ce saut aux fins de l'analyse visant à obtenir la valeur de vérification (VH) de cet ensemble d'instructions, et on vérifie ainsi le bon déroulement de cet ensemble d'instructions avant d'exécuter l'instruction de saut.

11. Procédé selon l'une quelconque des revendications 1 à 10, caractérisé en ce que l'on ré-initialise l'analyse avant chaque nouvelle surveillance d'une séquence ou d'un ensemble (EI1, EI2, EI3) d'instructions à surveiller.

12. Procédé selon la revendication 11, caractérisé en ce que la ré-initialisation de l'analyse à chaque nouvelle surveillance consiste à effacer ou remplacer une valeur de vérification (VH) obtenue lors d'une précédente analyse.

13. Procédé selon la revendication 11 ou 12, caractérisé en ce que la ré-initialisation de l'analyse de surveillance est commandée par le logiciel protégé lui-même.

14. Procédé selon l'une quelconque des revendications 1 à 13, caractérisé en ce que l'analyse produit une valeur de vérification (VH) obtenue en tant que dernière valeur d'une suite de valeurs que l'on fait évoluer successivement avec l'analyse de chacune des instructions (Inst.1-Inst.n) analysées de l'ensemble d'instructions, permettant ainsi de contenir un état interne du déroulement du procédé de surveillance et de suivre son évolution.

15. Procédé selon l'une quelconque des revendications 1 à 14, caractérisé en ce que l'analyse consiste à calculer (40, 42), pour chaque instruction considérée (Inst.n) succédant à une instruction précédente (Inst.n-1), le résultat d'une opération sur à la fois une valeur (VHn) obtenue de l'instruction considérée et le résultat (VHn-1) obtenu par la même opération effectuée sur l'instruction précédente.

16. Procédé selon l'une quelconque des revendications 1 à 15, caractérisé en ce que l'analyse consiste à appliquer de manière récursive une fonction de hachage f(VHn-1, Vinst.n) sur des valeurs obtenues de chaque instruction surveillée, en partant d'une dernière initialisation effectuée.

17. Procédé selon l'une quelconque des revendications 1 à 15, caractérisé en ce que l'analyse consiste à faire évoluer une valeur de vérification en effectuant un calcul de redondance non nécessairement cryptographique sur l'ensemble des codes d'opération et des adresses exécutées depuis la dernière initialisation effectuée.

18. Procédé selon l'une quelconque des revendications 1 à 17, caractérisé en ce que l'analyse consiste à obtenir une valeur de comparaison (VCn) par calcul de valeurs intermédiaires successives au fur et à mesure que l'on obtient les données des instructions respectives servant pour ce calcul durant l'exécution de ces instructions.

19. Procédé selon l'une quelconque des revendications 1 à 17, caractérisé en ce que l'analyse comprend une étape de sauvegarde de chaque donnée nécessaire pour la vérification, obtenue à partir des instructions de l'ensemble d'instructions à surveiller (Inst.1-Inst.n) au fur et à mesure qu'elles sont exécutées, et de n'effectuer un calcul de la valeur de vérification (VHn) à partir de ces données seulement au moment nécessaire, une fois que toutes les données nécessaires ont été obtenues.

20. Dispositif de surveillance du déroulement de l'exécution d'une suite d'instructions (Inst.1-Inst.n) d'un programme informatique mettant en œuvre le procédé de surveillance selon l'une quelconque des revendications 1 à 19, caractérisé en ce qu'il comprend des moyens (22-26) pour analyser la séquence des instructions transmises vers le processeur (4) destiné à exécuter le programme surveillé et des moyens (26) pour vérifier le résultat (VCn) de cette analyse par référence à des données de référence (Vréf) enregistrées avec ledit programme.

21. Dispositif selon la revendication 20, adapté pour mettre en œuvre le procédé de surveillance selon l'une quelconque des revendications 1 à 19, caractérisé

en ce qu'il comporte un registre (24) permettant d'enregistrer des résultats intermédiaires (VH) dans un calcul en chaîne effectué par le moyen d'analyse (26) pour obtenir une valeur de vérification (VHn).

22. Dispositif selon la revendication 21, caractérisé en ce qu'il comprend des moyens pour permettre l'enregistrement d'une valeur prédéterminée ou une remise à zéro du registre (24) sous la commande d'une instruction (Inst.n+1) transmise lors de l'exécution d'un programme à surveiller, par exemple à l'occasion d'un saut dans le programme.

23. Dispositif selon l'une quelconque des revendications 20 à 22, caractérisé en ce qu'il comporte un moyen (60) de comptabilisation du nombre de déroulements non-prévus du programme surveillé, tel que déterminé par le moyen d'analyse (26), et des moyens pour invalider l'utilisation future du programme à surveiller si ce nombre atteint un seuil (VCseuil) prédéterminé.

24. Dispositif selon l'une quelconque des revendications 20 à 23, caractérisé en ce qu'il est intégré à un dispositif programmé, telle qu'une carte à puce, contenant ledit programme à surveiller.

25. Dispositif selon l'une quelconque des revendications 20 à 23, caractérisé en ce qu'il est intégré un dispositif d'exécution de programme (20).

26. Dispositif d'exécution de programme (20), destiné à exécuter une suite d'instructions (Inst.1-Inst.n) d'un programme informatique, caractérisé en ce qu'il comporte des moyens (22-26) pour analyser la séquence des instructions transmises pour exécution et des moyens pour vérifier le résultat de cette analyse par référence à des données de référence (Vréf) enregistrées avec le programme à surveiller, selon l'une quelconque des revendications 20 à 23.

27. Dispositif d'exécution de programme (20) selon la revendication 26, adapté pour mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 21.

28. Dispositif programmé comportant une suite d'instructions enregistrées (Inst.1-Inst.n), caractérisé en ce qu'il comporte en outre une mémoire fixe contenant des données de référence (Vréf) préétablies en fonction de données contenues dans lesdites instructions et destinées à permettre une vérification de la séquence des instructions analysées selon l'une quelconque des revendications 1 à 21, ledit dispositif étant destiné à coopérer avec un dispositif de surveillance selon l'une quelconque des revendications 20 à 27.

29. Dispositif selon la revendication 28, caractérisé en ce qu'il se présente sous forme de carte à puce.

30. Dispositif selon la revendication 30 ou 31, caractérisé en ce que les données de référence (Vréf) sont enregistrées sous la forme de valeur(s) pré-câblée(s) fixée(s) en mémoire.

31. Dispositif de programmation d'un dispositif destiné à être programmé selon l'une quelconque des revendications 28 à 30, caractérisé en ce qu'il comprend des moyens pour inscrire à au moins un emplacement prédéterminé d'une séquence d'instructions du programme (Inst.1-Inst.n) une valeur de référence (Vréf) calculée selon un mode préétabli à partir de données comprises dans chaque instruction d'un ensemble d'instructions dont on souhaite surveiller l'exécution.

32. Machine virtuelle ou interpréteur interprétant un code critique, caractérisé en ce qu'il met en œuvre le procédé selon l'une quelconque des revendications 1 à 19 pour l'exécution de ce code critique.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 06 novembre 2000 (06.11.00)	
Demande internationale no PCT/FR00/00150	**Référence du dossier du déposant ou du mandataire** GEM0700
Date du dépôt international (jour/mois/année) 24 janvier 2000 (24.01.00)	**Date de priorité** (jour/mois/année) 09 mars 1999 (09.03.99)
Déposant GIRARD, Pierre etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

23 septembre 2000 (23.09.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

R. Forax

no de téléphone: (41-22) 338.83.38

"TRANSLATION OF ANNEX TO INTERNATIONAL PRELIMINARY EXAMINATION REPORT"

09/926174 Translation

77

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM0700	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00150	International filing date (*day/month/year*) 24 January 2000 (24.01.00)	Priority date (*day/month/year*) 09 March 1999 (09.03.99)
International Patent Classification (IPC) or national classification and IPC G06F 11/28		
Applicant GEMPLUS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 23 September 2000 (23.09.00)	Date of completion of this report 27 March 2001 (27.03.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/00150

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:
pages 1-23, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the claims:
pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-32, filed with the letter of 09 March 2001 (09.03.2001)

☒ the drawings:
pages 1/5-5/5, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☒ the claims, Nos. 33-34

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-32	YES
	Claims		NO
Inventive step (IS)	Claims	1-32	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-32	YES
	Claims		NO

2. Citations and explanations

1 The subject matter of **Claim 1** appears to be novel and inventive.

Claim 1 defines a method for monitoring the flow of execution of a linear series of program instructions.

The closest prior art, which is mentioned in the description, describes test methods aimed at avoiding unauthorised actions resulting from incorrect running of the program. Unauthorised actions are, for example, the disclosure of confidential data recorded in an electronic card or tampering with such data. In a test environment, these methods alter the value of the instruction counter using calculation modification or probing techniques. The altered instruction counter causes the program to run in an unexpected manner. If none of the events occurring during the unexpected running of the program causes an unauthorised action, then the running of the program meets the security requirements and is approved.

The closest prior art cited by the applicant uses the method whereby a plurality of erroneous values of the instruction counter are tested in order to ascertain whether the running of the program is the result of an unauthorised action. It is not possible to test all of the erroneous values of the instruction counter. Consequently, these test methods cannot prove that the running of the program does not result from any unauthorised action.

The method defined in **Claim 1** does not use the testing technique, but instead verifies that the linear series of instructions of a program has been executed in a linear manner. This verification involves extracting a data item from each instruction, performing a predetermined calculation on each data item thus extracted and comparing the result of the calculation with a predetermined reference data item. Consequently, the method defined in **Claim 1** ensures that the running of the program does not result from any unauthorised action.

Neither of the two documents cited in the international search report describes the verification of the execution of a linear series of instructions as defined in **Claim 1**.

The subject matter of **Claim 1** is therefore novel and inventive and satisfies the requirements of *PCT Article 33(2) and (3)*.

2 **Claims 2-19** are dependent on **Claim 1** and add further features to the inventive method of **Claim 1**. Consequently, the subject matter of **Claims 2-19** is

novel and inventive and satisfies the requirements of *PCT Article 33(2) and (3)*.

3. **Claim 20** concerns a device with technical features which make it suitable for carrying out the steps of the methods defined in **Claims 1-19**.
Claims 21-32 add further features to the device of **Claim 20**.
Consequently, the subject matter of **Claims 20-32** is novel and inventive and satisfies the requirements of *PCT Article 33(2) and (3)*.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM0700	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 00150	Date du dépôt international *(jour/mois/année)* 24/01/2000	(Date de priorité (la plus ancienne) *(jour/mois/année)* 09/03/1999
Déposant GEMPLUS et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 2 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

   [ ] le texte est approuvé tel qu'il a été remis par le déposant.

   [X] Le texte a été établi par l'administration et a la teneur suivante:

   ROCEDE DE SURVEILLANCE DU DEROULEMENT D'UN PROGRAMME

5. En ce qui concerne l'**abrégé**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n° 2

   [X] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 00/00150

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F11/28

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 4 266 272 A (BERGLUND ET AL.) 5 mai 1981 (1981-05-05) abrégé	1-34
A	EP 0 012 794 A (INTERNATIONAL BUSINESS MACHINES) 9 juillet 1980 (1980-07-09) abrégé	1-34

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
11 avril 2000	17/04/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Corremans, G

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/00150

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4266272 A	05-05-1981	BR 7906480 A	24-06-1980
		EP 0010123 A	30-04-1980
		JP 1261682 C	25-04-1985
		JP 55093600 A	16-07-1980
		JP 59038677 B	18-09-1984
EP 12794 A	09-07-1980	DE 2855865 A	26-06-1980
		JP 1322260 C	11-06-1986
		JP 55087253 A	01-07-1980
		JP 60049343 B	01-11-1985

CLAIMS

1. A method for monitoring progress with the execution of a series of instructions (Inst.1-Inst.n) in a computer program, consisting in analysing the sequence of instructions transmitted to the processor (4) intended to execute the program being monitored and to verify the result of this analysis by reference to reference data (Vref) recorded with the said program.

2. A method according to Claim 1, characterised in that the reference data comprise a value (Vref) pre-established so as to correspond to the result of this analysis produced during the monitoring method only if all the instructions (Inst.1-Inst.n) in the sequence of instructions have actually been analysed during the running of the program.

3. A method according to Claim 1 or 2, characterised in that the said analysis of the sequence of instructions (Inst.1-Inst.n) comprises the extraction (38) of a data item from each instruction transmitted to the processor (4) and a predetermined calculation (40, 42) on each data item thus extracted, and in that the verification comprises a comparison (50) of the result of the analysis with the reference data (Vref).

4. A method according to any one of Claims 1 to 3, characterised in that the said verification of the result of the analysis is caused by an instruction (Inst.n+1) placed at a predetermined location in the program to be monitored, this instruction containing

the reference data (Vref) relating to a set of instructions (Inst.1-Inst.n) whose correct execution is to be monitored.

5. A method according to any one of Claims 1 to 4, characterised in that, when the instructions (Inst.1-Inst.n) of the set of instructions to be monitored are in the form of a value, for example codes recorded in hexadecimal or decimal form, the said analysis of the instructions is carried out considering these as a numerical value.

6. A method according to Claim 1, comprising the steps consisting in:

- during the preparation of the program to be monitored:

  - incorporating, at at least one predetermined location in a sequence of instructions (Inst.1-Inst.n) in the program, a reference value (Vref) established according to a predetermined rule applied to identifiable data in each instruction to be monitored, and

- during the execution of the program to be monitored:

  - obtaining (38) the said identifiable data in each instruction received with a view to its execution,

  - applying (40, 42) the said predetermined rule to the said identifiable data thus obtained in order to establish a verification value (VHn), and

- verifying (50) that this verification value actually corresponds to the reference value recorded with the program.

7. A method according to any one of Claims 1 to 6, characterised in that it also comprises a step (56) of interrupting the flow of the program monitored if the analysis reveals that the program being monitored has not been run as expected.

8. A method according to any one of Claims 1 to 7, characterised in that it also comprises an invalidation step (70) for future use of the device comprising the monitored program if the said analysis reveals a predetermined number of times that the program being monitored has not run in the expected manner.

9. A method according to any one of Claims 1 to 8, characterised in that the set of instructions to be monitored does not include jumps in its expected flow.

10. A method according to any one of Claims 1 to 8, characterised in that, when the program (EI1, EI2, EI3) or the program portion to be monitored provides for at least one jump, the monitoring method is applied separately to sets of instructions in this program which do not include jumps between two successive instructions.

11. A method according to Claim 10, characterised in that, when the program to be monitored includes an instruction (EI1-j) giving rise to a jump dependent on the manipulated data, the monitoring method is implemented separately for a set of

instructions (EI1) which precedes the jump, and for at least one set of instructions (EI2, EI3) which follows this jump.

12. A method according to Claim 11, characterised in that, for a set of instructions (EI1) providing for a jump, there is integrated in this set the instruction (EI1-j) which controls this jump for the purpose of the analysis aimed at obtaining the verification value (VH) for this set of instructions, and thus the correct running of this set of instructions is verified before executing the jump instruction.

13. A method according to any one of Claims 1 to 12, characterised in that the analysis is reinitialised before each new monitoring of a sequence or set (EI1, EI2, EI3) of instructions to be monitored.

14. A method according to Claim 13, characterised in that the reinitialisation of the analysis of each new monitoring consists in erasing or replacing a verification value (VH) obtained during a previous analysis.

15. A method according to Claim 13 or 14, characterised in that the reinitialisation of the monitoring analysis is controlled by the protected software itself.

16. A method according to any one of Claims 1 to 15, characterised in that the analysis produces a verification value (VH) obtained as the last value in a series of values which is made to change successively with the analysis of each of the analysed instructions

(Inst.1-Inst.n) of the set of instructions, thus making it possible to contain an internal state of the running of the monitoring method and to follow its changes.

17. A method according to any one of Claims 1 to 16, characterised in that the analysis consists in calculating (40, 42), for each instruction under consideration (Inst.n) following on from a previous instruction (Inst.n-1), the result of an operation on both a value (VHn) obtained of the instruction in question and the result (VHn-1) obtained by the same operation performed on the previous instruction.

18. A method according to any one of Claims 1 to 17, characterised in that the analysis consists in recursively applying a hash function f(VHn-1, Vinst.n) to values obtained of each monitored instruction, starting from a last initialisation performed.

19. A method according to any one of Claims 1 to 17, characterised in that the analysis consists in making a verification value change by performing a redundancy calculation, not necessarily cryptographic, on all the operating codes and the addresses executed since the last initialisation carried out.

20. A method according to any one of Claims 1 to 19, characterised in that the analysis consists in obtaining a comparison value (VCn) by calculating successive intermediate values as the data of the respective instructions serving for this calculation during the execution of these instructions are obtained.

21. A method according to any one of Claims 1 to 19, characterised in that the analysis comprises a step of saving each data item necessary for verification, obtained from instructions in the set of instructions to be monitored (Inst.1-Inst.n) as they are executed, and performing a calculation of the verification value (VHn) from these data only at the necessary time, once all the necessary data have been obtained.

22. A device for monitoring progress with the execution of a series of instructions (Inst.1-Inst.n) of a computer program, having means (22-26) for analysing the sequence of instructions transmitted to the processor (4) intended to execute the program being monitored and means (26) for verifying the result (VCn) of this analysis by reference to reference data (Vref) recorded with the said program.

23. A device according to Claim 22, adapted to implement the monitoring method according to any one of Claims 1 to 21, characterised in that it has a register (24) for recording intermediate results (VH) in a calculation in a chain carried out by the analysis means (26) in order to obtain a verification value (VHn).

24. A device according to Claim 23, characterised in that it comprises means for allowing the recording of a predetermined value or a resetting of the register (24) under the control of an instruction (Inst.n+1) transmitted during the execution of a program to be monitored, for example on the occasion of a jump in the program.

25. A device according to any one of Claims 22 to 24, characterised in that it has a means (60) for counting the number of unexpected events in the program being monitored, as determined by the analysis means (26), and means for invalidating the future use of the program to be monitored if this number reaches a predetermined threshold (VCthreshold).

26. A device according to any one of Claims 22 to 25, characterised in that it is integrated into a programmed device, such as a smart card, containing the said program to be monitored.

27. A device according to any one of Claims 22 to 25, characterised in that it is integrated into a program execution device (20).

28. A program execution device (20) intended to execute a series of instructions (Inst.1-Inst.n) of a computer program, characterised in that it has means (22-26) for analysing the sequence of instructions transmitted for execution and means for verifying the result of this analysis by reference to reference data (Vref) recorded with the program to be monitored.

29. A program execution device (20) according to Claim 28, adapted to implement the method according to any one of Claims 1 to 21.

30. A programmed device containing a series of recorded instructions (Inst.1-Inst.n), characterised in that it also contains reference data (Vref) pre-established as a function of data contained in the said instructions and intended to allow verification of the

sequence of instructions analysed according to any one of Claims 1 to 21.

31. A device according to Claim 30, characterised in that it is in the form of a smart card.

32. A device according to Claim 30 or 31, characterised in that the reference data (Vref) are recorded in the form of a prewired value or values fixed in memory.

33. A device for programming a device intended to be programmed according to any one of Claims 30 to 32, characterised in that it comprises means for entering, at at least one predetermined location in a sequence of instructions in the program (Inst.1-Inst.n), a reference value (Vref) calculated according to a pre-established mode from data included in each instruction in a set of instructions whose execution it is wished to monitor.

34. A virtual machine or interpreter interpreting a critical code, characterised in that it implements the method according to any one of Claims 1 to 21 for the execution of this critical code.